HP MSM7xx Controllers v5.7.0.3 Release Notes

HP Part Number: 5998-3346
Published: June 2012
Edition: 2

Acknowledgements

Windows® is a U.S. registered trademark of Microsoft Corporation.

Version: MSM v5.7.0.3

Description

These Release Notes provide important release-related information.

NOTE: In this document, except when identifying specific models, the generic term "controller" is used in place of MSM7xx Controller product names and the generic term "AP" is used in place of MSM3xx / MSM4xx AP product names.

Product models

This document applies to these HP products:

Model	Part
MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
E-MSM720 Access Controller	J9693A
E-MSM720 Premium Mobility Controller	J9694A
E-MSM720 Access Controller (TAA)	J9695A
E-MSM720 Premium Mobility Controller (TAA)	J9696A
MSM760 Access Controller	J9421A
MSM760 Premium Mobility Controller	J9420A
MSM765zl Premium Mobility Controller	J9370A

NOTE: Software version 5.7.0.3 is not intended for use in Japan. MSM APs and MSM Controllers in Japan must use software version 5.7.0.4 or higher and not v5.7.0.3. Please consult the v5.7.0.4 Release Notes.

Online documentation

You can download documentation from the HP Support Website at: www.hp.com/support/manuals. Search by product name or part number.

Software Updates and Licensing portal

The Software Updates and Licensing portal provides access to the latest software updates to customers with a support contract. An HP Passport is required to access the Software Updates and Licensing portal at www.hp.com/go/hpsoftwareupdatesupport and it is available to customers who have purchased a maintenance and support agreement.

Updating software

Update the controller software as described in the "Software updates" section of the *MSM7xx Controllers Configuration Guide*. Once the controller is updated, it automatically updates all of its controlled devices to the same software version.

MSM management tool now requires web browser with SSLv3 support

NOTE: Starting with MSM software version 5.7.0.3, a web browser that supports SSLv3 is mandatory for running the MSM web-based management tool. SSLv3 is supported by Microsoft Internet Explorer 7 and 8 but must be enabled. Microsoft Internet Explorer 9 only uses SSLv3. Mozilla Firefox also supports SSLv3 but support may need to be enabled or you may need to update to a more recent version.

Configuring Teaming on the E-MSM720

For important information on how to configure Teaming on the E-MSM720, consult these sections in the *MSM7xx Controllers Configuration Guide*:

- "Teaming two E-MSM720s using the Access network or Internet network"
- "Teaming two E-MSM720s using a direct link"

Note also that these sections in the *MSM7xx Controllers Configuration Guide* supersede E-MSM720 teaming-related information in the management tool online help.

GMS (Guest Management Software)

MSM7xx Controllers purchased on April 15, 2010 or later, are entitled to GMS. MSM7xx Controllers with an active software support contract are also entitled to GMS.

HP GMS simplifies centralized guest-account creation from any Microsoft Windows-based computer. It provides centralized, real-time management of visitor accounts and sessions with a configurable visitor session duration per account. The intuitive user interface is designed for receptionists and clerical staff with minimal training. Working with HP MSM7xx Controllers, secure login prevents unauthorized account creation, and the reporting feature records all account management activity for audits. A digital certificate secures all communications between GMS and the MSM7xx Controller. For details and download instructions, consult the *Guest Management Software (GMS) v5.7.x Release Notes*. Search for "Guest Management Software" at www.hp.com/support/manuals.

NOTE: GMS 5.7.0.1 works with MSM software versions 5.7.0.x up to and including version 5.7.0.2. GMS 5.7.0.3 is required for MSM software version 5.7.0.3 and higher.

NOTE: GMS 5.7.0.x does not support interaction with MSM7xx Controller teams. GMS 5.7.0.x must only be used with standalone MSM7xx Controllers.

RF Manager software and MSM software version compatibility

RF Manager versions 5.9.x and 6.0.x work with MSM software version 5.5.x and higher. However, to use the WLAN Integration feature in RF Manager 6.0.x, the RF Manager and MSM software versions must be matched as follows:

MSM7xx software version	Compatible RF Manager version(s)	Sensor devices version	
		Sensor-only devices (MSM415)	AP/Sensor combo devices (MSM320*, MSM325, MSM335)
5.7.0.2/5.7.0.3	6.0.162 or above	Upgraded automatically by RF Manager	Upgraded automatically by MSM7xx Controller
5.5.3.x	6.0.157 or above		
5.5.1.x/5.5.2.x	6.0.154 or above		
5.5.0.x	5.9.203, 6.0.147 or above		

*MSM320 APs that have been upgraded to MSM325 RF sensor via HP MSM320 RF Sensor License J9384A.

NOTE: If with RF Manager 6.0.x you choose to use mismatched software versions, you should first turn off the WLAN Integration in RF Manager.

NOTE: Upgrading an MSM7xx Controller to v5.7.0.3 will also automatically upgrade any MS325 and MSM335 Sensors it manages to v5.7.0.3.

NOTE: The MSM415 Sensor has no MSM software dependency. It is managed and upgraded directly by RF Manager.

PCM+ (PCM/MM/IDM) software support

PCM+ (PCM/MM/IDM) version 4.0 or higher is required to support MSM devices at software version 5.7.x. Purchase of PCM+ does not entitle you to MSM product software upgrades. Except for the MSM720, only MSM products covered by a care pack or contract that includes software upgrades are entitled to upgrades.

Clear web browser cache before launching management tool

In the management tool the Automated Workflow pages use updated JavaScript files. If your web browser cache contains old versions of these files you may see JavaScript errors. If this occurs, clear your web browser cache and re-launch the management tool.

Fixes

The following issues are fixed in this release:

- (Applies to MSM710.) When the number of adopted APs reaches the controller limit, the controller restarts.
- The 802.1X reauthentication default time is too short (3 seconds) for some mobile devices. It has been increased to 30 seconds.
- The management tool cannot be used properly in Microsoft Internet Explorer 9.
- When a wireless client authenticates to an 802.1x VSC, the AP fails to complete the encryption handshake and terminates the session.
- (Applies to MSM710, E-MSM720.) When the controller starts up, a database read error may occur. A message similar to this appears in the system log: `iappd_sc PostMobilityClient: Failed to read local SC [] data from database`.
- Two (or more) wireless clients connected to the same VSC but configured to egress traffic on different VLANs are able to communicate with each other. This should not be the case.
- When the controller internal RADIUS server is under heavy load (200 or more users authenticating simultaneously), RADIUS authentication fails for some users. A message similar to this appears in the system log: `...radius exceeds data memory`.
- (Applies to a pre-v5.7.x controller team (MSM760 or MSM765zl) having its software upgraded to v5.7.0.x.) In some cases, upgrading a controller team may cause teaming to become inoperative. When this occurs, team members will fail to synchronize with the team manager, and the status of team members on the team manager will be shown as either **Resetting configuration** or **Applying configuration**.
- (Applies to pre-v5.7.x MSM760/MSM765zl controller teams configured to perform centralized user authentication.) Although the number of locally homed user accounts that are supported on the controllers is greater than 100 (as per documentation), after upgrading to v5.7.0.x with the number of user accounts configured exceeding 100, the teaming transaction times out and causes the member controller to fail to synchronize its configuration with the team manager.
- Controller team members restart when the team manager returns after failover. If a team manager becomes inoperative and is replaced by an alternate manager for at least five minutes, then five

to ten minutes after the manager returns from failover, all team members restart, interrupting wireless service.

- APs located 16 or more hops away from a DHCP server may become unreachable by the controller due to timeouts.
- When using the internal RADIUS server, the controller does not keep track of queued EAPOL requests, causing some clients to be unable to authenticate.
- When Security filters are not enabled in a VSC, wireless clients connected to the same VSC and with the same egress VLAN, cannot communicate with each other.
- (Applies to teaming with E-MSM720, MSM760, MSM765zl.) When 802.11n MCS rates are disabled in a VSC, team member controllers fail to synchronize with the team manager controller.
- (Applies to 802.1X authentication with local RADIUS server.) Sessions time out too quickly, requiring users to re-log in.
- When wireless clients authenticate with an external RADIUS server with the controller acting as a RADIUS client, the controller generates duplicate RADIUS ID in the packets, causing the RADIUS server to terminate the user session.
- When there are usernames longer than 96 characters, the Wireless Client Overview page stretches the Username column, making other columns unreadable.
- After 802.1X settings in a VSC are changed and synchronized to controlled APs, some of the APs fail to synchronize and remain in the "Restoring config" state.
- (Applies to E-MSM720, MSM760, MSM765zl.) When the number of access points adopted by a team is high (approaching the team limit), the exchange of statistics between the controller and the APs causes some APs to restart.
- When the number of Mobility Traffic Manager (MTM) clients grows beyond 500, some of the APs may restart. A message similar to the following appears in the system log: `... warning monitord monitord: CN13DLL03G Unexpected termination for process 'iappd -d -m 169.254.0.1 -t 10.14.0.36' [pid 29720, up for 2 sec(s)]`
- When configuring an AP with two Mobility Traffic Manager (MTM) VSCs with the same settings but different names and SSIDs on radios 1 and 2 respectively, clients lose connectivity when roaming between radios.
- When the number of simultaneous connected clients approaches the maximum number permitted, high CPU utilization is experienced, possibly causing a controller restart. The system log indicates that “iappd" is consuming the CPU.
- Some traffic from a client connected to an access-control VSC (tunneled between the access point and the controller) is detected at the switch where the access point is connected.
- All wireless client sessions are unexpectedly dropped simultaneously.
- (Applies to E-MSM430, E-MSM460, E-MSM466, E-MSM466-R.) Controller based provisioning with local mesh connectivity does not work properly at the AP Group or and Controlled APs levels.
- When a VSC is configured for non-access controlled 802.1X authentication with a remote RADIUS server, even if the authentication is successful, the controller generates messages similar to this in the system log: `iprulesmgr Discarding RADIUS Packet (Length:'44',Code:'Access-Reject',Id:'87') from RADIUS Server (Ip:'x.x.x.x',Port:'xxxx') due to authentication failure (check shared secret configuration)`

Known teaming issues

The following teaming-related issues are present in this release:

- (Applies to Teaming with E-MSM720, MSM760, MSM765zl.) When roaming from an AP managed by the team manager to another AP managed by a team member, wireless clients may experience a delay of up to 15 seconds when trying to reach other wireless clients on the same VSC.
- When the system time is set manually, if the team manager controller is shut down (power disconnected) when the team manager controller returns, the team manager controller time is set to the last saved time, which may cause team member controllers to fail to re-synchronize with the team manager controller. As a workaround, Use an NTP service on the network for automatic system time setting.
- When upgrading from 5.4.x or 5.5.x to 5.7.x, depending on the settings already in the configuration file, messages similar to the following may appear in the system log after the upgrade is complete. In this context, such messages can generally be safely ignored.

```
Apr 19 14:32:38 err monitord   Upgrade 200 failed: Unable to get IGMP inheritance section inside AP-1: 3
Apr 19 14:32:38 debug monitord Performing upgrade 201 (v13.4 reference:QC55390-QC42402). Required to update
current version 10.22 to 13.5.
Apr 19 14:32:38 err monitord   Upgrade 201 failed: Failed to update provisioning phytype token: 3
Apr 19 14:32:39 err monitord   Upgrade process error: Some upgrade scenarios failed.
```

- When a controller team attempts to manage the maximum number of APs as defined in its installed AP licenses, it may trigger one or more team members to restart. For example, assume a team has a total of 100 AP licenses installed. When the team attempts to manage the 100th AP, one or more team members may restart. To avoid this issue, keep the number of installed APs below the maximum number of installed licenses.
- (Applies to E-MSM720 with Teaming.) The message "Firmware unavailable" may appear for the team member controller. As a workaround, use the management tool to re-install v5.7.x software on the team manager controller.
- (Applies to E-MSM720, MSM760, MSM765zl.) GMS 5.7.0.x does not support interaction with MSM7xx Controller teams. GMS 5.7.0.x must only be used with standalone MSM7xx Controllers.
- (Applies to E-MSM720, MSM760, MSM765zl with teaming and Mobility Manager.) After a failover to a team member controller has occurred, the Mobility Manager dashboard becomes unable to display correct information for the team. To display the correct information, the teamed controllers must be restarted, ensuring that the new master controller boots first.
- (Applies to PCM interacting with APs controlled by an MSM7xx Controller team.) You cannot use PCM to manually disable sampling and statistics for active sFlow agents on MSM APs controlled by a team. As a workaround, use the management tool on the team master, and disable the AP sFlow agent on page **Controller >> Tools > sFlow**.
- Creating a mobility domain between a team of controllers (that use a VLAN for teaming communication) and another controller is not working properly if the team is set as the primary mobility controller. In this case the IP address of the slave controller is not properly set on the mobility domain. To avoid this, set the other controller (not the team) as the primary mobility controller.
- (Applies to Japan (JP) versions of MSM320 with an MSM7xx Controller team.) Upon team failover to a team member, the MSM320 shows as having incompatible settings when attempting to re-synchronize with the team member.

- (Applies to E-MSM720, MSM760, MSM765zl with Teaming.) A controller that has DNS discovery settings defined on the **Controlled APs >> Provisioning > Discovery** page may be unable to synchronize with a team in the following two scenarios:
  - If the team members have different DNS discovery settings configured, the controller will not be able to synchronize.
  - If the team initially has no DNS discovery settings configured, the controller will be able to synchronize, however, if the DNS settings on the team are then changed, the controller will no longer be able to synchronize.
- (Applies to MSM760, MSM765zl with teaming enabled.) When opening the AP Overview page with more than 300 APs, the management tool may stop working, requiring it to be re-launched.
- (Applies to E-MSM720, MSM760, MSM765zl.) Teaming redundancy is not implemented for the sFlow feature. Therefore, upon master controller failover to a team member, sFlow will be shown as disabled on the team member that is temporarily filling the master role. As a workaround, manually configure the team, enabling the temporary master as the real master controller, and enabling sFlow on this master controller.
- On a controller team, if a VSC has the **DHCP relay agent** feature enabled with the **Subnet selection** option, the relay does not work properly when the team manager recovers after a shutdown.

Other known issues

These other issues are present in this release:

- (Applies to E-MSM720, MSM760, MSM765zl.) When a mobility domain grows and includes many (more than 10) controllers (either teamed or standalone), Mobility Traffic Manager (MTM) clients roaming from one controller to another may randomly drop their connection or experience delays in recovering wireless service.
- When a controlled AP configuration is updated after a MAC address is added or removed from the allowed stations list, other wireless clients associated with the same VSC lose connectivity until they are reauthenticated. As a workaround, reauthenticate the wireless clients.
- When a controller is handling live streaming traffic from many wireless users, the controller management tool may become temporarily unreachable. As a workaround, consider using the CLI interface or wait for the heavy traffic to subside.
- Wireless clients connected to an AP adopted on the controller Internet interface are not able to ping and communicate with other wireless clients on the same VSC that are connected to an AP adopted on the controller LAN interface. As a workaround, use IP routes or external routing mechanisms.
- The **Save** button on management tool page **Controller > VPN > L2TP server** does not apply the configuration settings. As a workaround, use alternative configuration interfaces (CLI, SOAP, SNMP).
- When a second VSC is added, wireless clients on the first VSC are not able to ping each other (although wireless clients can ping their default gateway and retain network connectivity).
- (Applies to MSM760.) The Internet port cannot be manually set to 10 Mbps full duplex. Auto settings work as expected
- (Applies to MSM422 acting as a Slave in a Local Mesh configuration.) If the AP was directly provisioned before being adopted by a controller, the AP will not synchronize with the controller. This may be caused by a specific configuration were the Alt-Master only has the Local mesh provisioning profile enabled rather than having an additional Local mesh profile for the slave(s).
- EAP outer usernames longer than 96 characters are truncated by the AP before they are forwarded to an external RADIUS server. As a workaround, enable support for Anonymous outer usernames

on the RADIUS server. Note that the AP does not truncate the inner username used by the EAP method.

- (Applies to E-MSM720.) On page **Network > Address Allocation**, The **Max Connections** parameter under **VPN address pool** has an incorrect default value of 55. When attempting to save changes to this page, an error message will appear indicating that **Max Connections** must have a value in the range of 1 to 15. As a workaround, change **Max Connections** to a number in the range of 1 to 15.
- When sFlow is enabled, it cannot be disabled unless there is at least one controlled AP.
- (Applies to E-MSM720.) In the HP MSM MIBs, a query to **sysObjectID.0** returns **colubrisProducts.56** instead of the correct value **colubrisMSM720**.
- The DHCP Relay agent incorrectly uses source port 67 when forwarding DHCP broadcasts to DHCP Servers causing some DHCP servers to ignore the requests.
- The **show config** CLI command generates an **unable to read configuration** error in the management tool syslog.
- (Applies to MSM760, MSM765zl.) Associating or authenticating a wireless client with a VPN-based login VSC that uses L2TP over IPSec may cause the controller to restart. As a workaround, use PPTP over IPSec.
- If the **DHCP server**/**DHCP relay agent** option is configured in a VSC (cannot be the default VSC) and then **Access control** is cleared in the VSC, the DHCP server/DHCP relay agent option is not disabled. This causes the routing table to still be populated even though the option is no longer used. Instead, disable the **DHCP server**/**DHCP relay agent** in the VSC before clearing the **Access control** option.
- When adding an IPSec policy, the **NAT** option under Security Policy can not be enabled if the **Accept any peer** option is enabled under Peer Information. The only way to enable NAT in this context is to clear the **Accept any peer** option and to enable **Tunnel** under **General > Mode**.
- (Applies to MSM410, E-MSM430, E-MSM460, E-MSM466.) Due to a software design change, 802.11 LEAP authentication (some devices use terminology such as “Network EAP”) is no longer supported.
- (Applies to MSM710, E-MSM720, MSM760.) Communications problems may occur if the controller and any connected Ethernet switch both have manual Duplex and Speed settings, even when the settings match. As a workaround, set at least the MSM7xx Controller to **auto** for both Duplex and Speed.
- (Applies to HTML authentication on an access-controlled VSC with Active Directory as the authentication server.) Authenticated users are not displayed on the **Controller > Controlled APs >> Overview > Wireless clients** page.
- When MAC-based authentication is configured for both Local and Remote RADIUS server, the NAS-ID is omitted for the remote RADIUS server.
- When a VSC is configured for Mobility Traffic Manager (MTM) (non-access-controlled) and MAC-based authentication is set for both Local and Remote RADIUS servers, the Remote RADIUS server will never be queried even if no match if found in the local database.
- In cases where there are more than one controller sharing the same egress VLAN for an Access-Controlled VSC, and the **DHCP relay** and **Extend VSC egress subnet to VSC ingress subnet** options are enabled, it is possible that the same IP address will be active on more than one controller at the same time, causing more than one controller to answer ARP requests for this IP address, leading to incorrect behavior. To avoid this when more than one controller is sharing the same egress VLAN, set DHCP lease time to at least 10 minutes.
- (Applies to MSM410, E-MSM430, E-MSM460, E-MSM466, E-MSM466-R.) If a radio Channel setting of **Automatic** is enabled and all APs (affected by this issue) happen to boot up at the same time, for example after a power outage, then they are likely to end up on the same channel. This

will happen mostly with autonomous APs. APs managed by an MSM7xx Controller are less likely to experience this. As a workaround, APs can be restarted/re-synchronized at specific intervals or fixed channels can be selected.

- (Applies to E-MSM720.) The **L2TP** option for VPN Based Authentication is not supported in this release.
- (Applies to E-MSM720.) IPSec is not supported in this release.
- (Applies to MSM310, MSM320, MSM325, MSM335, MSM422.) Sometimes an Apple Mac Book is unable to forward traffic to the external network even though the wireless signal is shown as Excellent. Furthermore, the AP wireless driver may stop working. Either restart the AP or re-synchronize it after a radio configuration change.
- When a less specific static route is configured after a more specific static route has been configured, the controller forwards packets incorrectly.
- (Applies to E-MSM430, E-MSM460, E-MSM466, E-MSM466-R.) Dynamic VLAN assignment fails, causing user traffic to be placed onto the default network, preventing users from getting an IP address on the correct subnet.
- When a Mobility Traffic Manager (MTM) user is assigned to network mapped to a VLAN range, the selected VLAN ID within the range may change when users roam. To avoid this, do not use VLAN ranges.
- (Applies to E-MSM720 with Mobility Traffic Manager (MTM).) Egressing traffic on the Internet network and Access network is not supported. Egressing traffic onto a user-created network profile is supported.
- When setting the SNMP Syslog trap level below **Warning**, no traps will be generated.
- When an access-list is created to enable a proxy server using HTTPS, wireless clients may be unable to gain access to the secure site. As a workaround, restart the controller to activate the access list.
- The management tools allows the Metric value for gateways to be set to 0. Ensure that you set a gateway metric to a value other than 0.
- (Applies to MSM410.) You need to add an extra VLAN to pass traffic over a local mesh link in controlled mode. In earlier MSM410 software versions you could discover and pass data over the same VLAN. You now cannot send data over the discovery VLAN. You must add another VLAN for data traffic.
- Static NAT mappings are incorrectly limited to a maximum of 63 via the CLI and 200 via the management tool.
- (Applies to E-MSM720.) There is no Spanning Tree Protocol (STP) loop protection so avoid interconnecting two or more ports that are on the same VLAN.
- Active Directory (AD) users of a VSC configured for HTML authentication cannot log in if both Local and Remote (Active Directory) is enabled. This will still work if only Remote is enabled.
- VPN-based IPSec clients are unable to connect to MSM7xx Controllers, resulting in display of messages similar to this: **XAUTH wrong UserId or Password**.
- The maximum quantity of CA certificates and Client certificates that can be installed on the system is 50 certificates each. In some cases when adding more than 45 certificates of either type, the certificate names may disappear and an access error may be generated when selecting a different management tool menu. As a workaround, restart the controller.
- On the E-MSM720 there is no SNMP MIB support for Port Trunking.

- (Applies to USA and Canada.) System Time is not being set back one hour when DST ends at 2:00 a.m. on the first Sunday in November.
- If you configure the local DHCP server on a VSC to operate on the subnet 192.168.1.x/ 24, the route for users on this subnet will be deleted if the controller is restarted. The subnet 192.168.1.x/24 should not be used by a DHCP server on a VSC.